INDUSTRY LEADERSHIP TIP CARD

As a business leader, it is important to constantly be cyber-aware and incorporate cyber safety into your business strategy. Employees will look to leadership for best practices and proper execution of safe cybersecurity habits. By practicing healthy cybersecurity hygiene now, your business will have a better chance of avoiding compromised systems and lost profits.

DID YOU KNOW?

- The yearly cost of cyber crime per organization spanned a range of **$1.3 million to $58 million**.[1]
- The cost of cyber crime increased **26 percent,** or **$2.6 million** from 2012 to 2013.[2]

SIMPLE TIPS

1. Implement a layered defense strategy that includes technical, organizational, and operational controls.
2. Establish clear policies and procedures for employee use of your organization's information technologies.
3. Coordinate cyber incident response planning with existing disaster recovery and business continuity plans across your organization.
4. Implement technical defenses, such as firewalls, intrusion detection systems, and Internet content filtering.
5. Update your anti-virus software often.
6. Follow your organization's guidelines and security regulations.
7. Regularly download vendor security patches for all of your software.
8. Change the manufacturer's default passwords on all of your software.
9. Encrypt data and use two-factor authentication where possible.
10. If you use a wireless network, make sure that it is secure.
11. Monitor, log, and analyze successful and attempted intrusions to your systems and networks.

[1] 2013 Cost of Cyber Crime Study: United States, Ponemon Institute, October 2013

[2] Ibid

RESOURCES AVAILABLE TO YOU

US-CERT.gov

The United States Computer Emergency Readiness Team (US-CERT) has numerous tips and resources on topics like choosing and protecting passwords, email attachments, and safely using social networks.

FBI.gov

The Federal Bureau of Investigation leads the national effort to investigate high-tech crimes, including cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber crimes.

Cybercrime.gov

The Department of Justice component responsible for implementing national strategies in combating computer and intellectual property crimes worldwide.

StaySafeOnline.org

The Stop.Think.Connect.™ Campaign is a cooperative agreement between the Department of Homeland Security and the National Cyber Security Alliance (NCSA). Get more information about the Stop.Think.Connect. Messaging Convention, which is the formal way industry participates in the Campaign.

NIST.gov/CyberFramework

The National Institute of Standards and Technology developed the Framework for Improving Critical Infrastructure Cybersecurity. The Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure and help owners and operators of critical infrastructure manage cybersecurity-related risk.

Critical Infrastructure Cyber Community C^3 Voluntary Program

The Critical Infrastructure Cyber Community C^3 Voluntary Program is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes through the use of the Framework.

IF YOU'VE BEEN COMPROMISED

- Follow your organizations rules and regulations regarding cyber threats.
- Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov.
- Inform local law enforcement as appropriate.
- Report stolen finances or identities and other cyber crimes to the Internet Crime Complaint Center at www.ic3.gov.
- Report fraud to Federal Trade Commission at www.onguardonline.gov/file-complaint.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and you community. For more information visit http://www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™